瞭解Catalyst 3550上的QoS管制和標籤

目錄

簡介

策略功能確定流量級別是否在指定的配置檔案或約定範圍內，並允許您捨棄配置檔案外流量，或將其標籤為不同的差分服務代碼點(DSCP)值。這強制實施合約服務水準。

DSCP是封包的服務品質(QoS)等級的量度。除了DSCP，IP優先順序和服務類別(CoS)也用於傳送封包的QoS層級。

策略不應與流量整形混淆，儘管二者都確保流量保持在配置檔案或約定範圍內。

管制不會緩沖流量，因此管制不會影響傳輸延遲。策略不是緩衝超出配置檔案的資料包，而是丟棄這些資料包或使用不同的QoS級別（DSCP降級）對其進行標籤。

流量整形會緩衝超出配置檔案的流量並使突發流量平滑，但會影響延遲和延遲變化。整形只能應用於傳出介面，而策略可在傳入和傳出介面上應用。

Catalyst 3550支援傳入和傳出方向的管制。不支援流量調節。

標籤根據策略更改資料包QoS級別。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

硬體和軟體版本

所有軟體版本都支援Catalyst 3550上的管制和標籤。此處列出了最新的配置指南。請參閱本文檔瞭解所有支援的功能。

- 配置QoS

QoS管制和標籤引數

為了設定管制，必須定義QoS策略對映並將其應用於埠。這也稱為基於埠的QoS。

附註： Catalyst 3550目前不支援基於VLAN的QoS。

策略器由速率和突發引數以及針對配置檔案外流量的操作定義。

支援以下兩種型別的策略器：

- 聚合
- 個人

聚合策略器對應用該策略的所有例項中的流量執行操作。各個策略器對應用它的每個例項上的流量單獨起作用。

注意：在Catalyst 3550上，聚合管制器只能應用於同一策略的不同類。不支援跨多個介面或策略進行聚合管制。

例如，應用聚合管制器，將同一策略對映中類customer1和類customer2的流量限製為1 Mbps。此類管制器允許customer1和customer2兩個類中的1 Mbps流量。如果應用單個管制器，管制器將customer1類的流量限製為1 Mbps，將customer2類的流量限製為1 Mbps。因此，監察器的每個例項都是獨立的。

下表總結了當入口和出口策略都處理資料包時，對資料包執行的QoS操作：

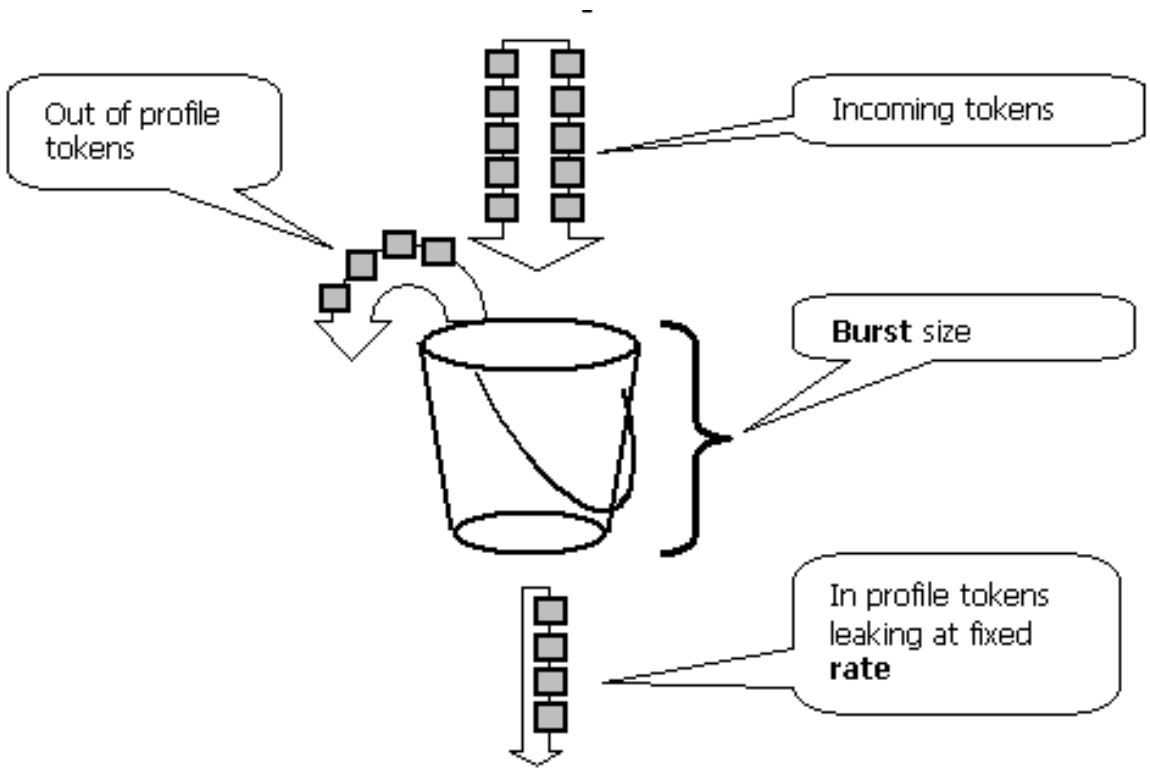
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

注意：可以在同一策略的同一流量類中進行標籤和降級。在這種情況下，特定類的所有流量都首先標籤。對已標籤的流量執行管制和降級。

Catalyst 3550中的QoS管制符合以下漏桶概念：

與傳入流量資料包大小成比例的令牌數量被放入令牌桶中；令牌數等於資料包的大小。以常規間隔，從桶中移除從配置的速率衍生的已定義數量的令牌。如果儲存桶中沒有位置容納傳入資料包，則會認為資料包超出配置檔案範圍並根據配置的策略操作將其丟棄或降級。

此概念如以下範例所示：



注意：流量不會快取在儲存桶中，因為它可能出現在此示例中。實際流量根本不會流經桶；bucket僅用於決定封包是否在設定檔中，或是超出設定檔。

注意：管制的硬體實施可能有所不同，但在功能上仍符合此模型。

這些引數控制策略的操作：

- **Rate** — 定義在每個間隔移除的令牌數。這有效地設定了管制速率。低於該速率的所有流量都會在配置檔案中考慮。支援的速率範圍為8 Kbps到2 Gbps，增量為8 Kbps。
- **Interval** — 定義令牌從桶中刪除的頻率。間隔固定為0.125毫秒（或每秒8000次）。 此間隔無法更改。
- **突發**(Burst) — 定義儲存段在任何時間可以容納的最大令牌數。支援的突發流量範圍從8000位元組到2000000位元組，增量為64位元組。

注意：雖然命令列幫助字串顯示大量值，但是rate-bps選項不能超過配置的埠速度，突發位元組選項不能超過2000000位元組。如果輸入的值較大，交換機會在您將策略對映連線到介面時將其拒絕。

為了維持指定的流量速率，突發必須不小於以下等式的總和：

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

例如，計算最小突發值以維持1 Mbps的速率。速率定義為1000 Kbps，因此所需的最小突發量是以下公式的總和：

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

支援的最小突發大小為8000位元組，大於計算的最小突發大小。

註：由於硬體策略粒度，準確的速率和突發量將舍入到最接近的支援值。

設定突發速率時，必須考慮到某些通訊協定實作對封包遺失作出反應的機制。例如，傳輸控制通訊協定(TCP)將每個遺失封包的視窗減少一半。當TCP嘗試加速到線路速率並被管制器限制時，這會導致TCP流量出現「鋸齒狀」效應。如果計算鋸齒業務量的平均速率，則該速率遠低於管制速率。但是，您可以增加突發量，以便獲得更好的利用率。一個良好的開端是設定突發量，使其等於來回時間(TCP RTT)期間以所需速率傳送流量的兩倍。 如果RTT未知，則可以將突發引數的值加倍。

出於同樣的原因，建議不要根據面向連線的流量來設定監察器操作的基準。此方案通常顯示低於策略器所允許的效能。

無連線流量也可以以不同的方式響應策略。例如，網路檔案系統(NFS)使用區塊，這些區塊可能包含多個使用者資料包通訊協定(UDP)封包。丟棄一個資料包可能會觸發多個資料包（甚至整個塊）重新傳輸。

此範例會計算具有64 Kbps管制速率且給定TCP RTT為0.05秒的TCP作業階段的突發量：

```
<burst> = 2*  *  = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800    [bytes]
```

在本例中，<burst>一個TCP作業階段。將此數值擴展為通過監察器的預期會話的平均數。

注意：這只是一個示例，在每種情況下，您需要評估流量和應用要求以及行為與可用資源的對比，以便選擇策略引數。

策略操作可以是丟棄資料包或更改資料包的DSCP（降級）。 為了降級資料包，必須修改受管制的DSCP對映。預設管制的DSCP對映將資料包註釋到同一個DSCP。因此，不會發生降價。

當將超出配置檔案的資料包標籤為對映到與原始DSCP不同的輸出隊列的DSCP時，資料包可能會順序混亂。如果資料包的順序非常重要，請將超出配置檔案的資料包降級為對映到與內配置檔案資料包相同的輸出隊列的DSCP。

Catalyst 3550支援的管制和標籤功能

下表彙總了Catalyst 3550支援的管制和標籤相關功能，並依方向分類：

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

每個類對映支援一個match語句。以下是輸入策略的有效match語句：

- match access-group
- match ip dscp
- match ip precedence

注意：在Catalyst 3550上，不支援**match interface命令，且類別對映中只允許有一個match命令。**因此，對通過介面傳入的所有流量進行分類並使用單個監察器對所有流量進行監察非常困難。請參閱本檔案的如何使用單一管制器對所有介面流量分類。

這是出口策略的有效match語句：

- match ip dscp

以下是輸入策略的有效策略操作：

- 警察
- set ip dscp（標籤）
- set ip precedence(marking)
- 信任dscp
- trust ip-precedence
- 信任cos

下表顯示了支援的輸入QoS策略矩陣：

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. 此選項還包括匹配IP優先順序。
2. 此選項涵蓋信任CoS、IP優先順序和DSCP。
3. 此選項還包括設定IP優先順序。

這是出口策略的有效策略操作：

- 警察

此表顯示了支援的出口QoS策略矩陣：

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

標籤允許資料包的QoS級別根據分類或策略進行更改。分類根據定義的標準將流量劃分為不同的類別以進行QoS處理。

QoS處理基於內部DSCP;資料包的QoS級別的度量。根據信任配置派生內部DSCP。系統支援信任的CoS、DSCP、IP優先順序和不受信任的介面。Trust指定為每個資料包派生內部DSCP的欄位，如下所示：

- 信任CoS時，QoS層是從交換器間連結通訊協定(ISL)或802.1Q封裝封包的第2層(L2)標頭派生的。
- 當信任DSCP或IP優先順序時，系統相應地從資料包的DSCP或IP優先順序欄位匯出QoS級別。

信任CoS僅對中繼介面有意義，而信任DSCP（或IP優先順序）僅對IP資料包有意義。

當介面不受信任時，內部DSCP從相應介面的可配置預設CoS中匯出。這是啟用QoS時的預設狀態。如果未配置預設CoS，則預設值為零。

確定內部DSCP後，可通過標籤和策略對其進行更改，或保留。

封包進行QoS處理後，其QoS層級欄位(在IP的IP/DSCP欄位內，以及ISL/802.1Q標頭（如有）內)會從內部DSCP更新。以下與管制相關的特殊QoS對應：

- **DSCP-to-Policed DSCP** — 用於在降級資料包時派生管制的DSCP。
- **DSCP-to-CoS** — 用於從內部DSCP匯出CoS級別，以更新傳出資料包ISL/802.1Q報頭。
- **CoS-to-DSCP** — 用於在介面處於信任CoS模式時從傳入CoS（ISL/802.1Q報頭）派生內部DSCP。

以下是特定於實施的重要注意事項：

- 當介面配置為信任任何QoS指標（例如CoS/DSCP或IP優先順序）時，不能將入口服務策略附加到介面。為了在DSCP/IP優先順序上匹配並在入口上執行police，您必須為策略中的特定類配置信任，而不是在介面上。要根據DSCP/IP優先順序進行標籤，必須配置信任。
- 從硬體和QoS的角度來看，只有沒有IP選項和乙太網II高級研究專案機構(ARPA)封裝的IPv4流量才被視為IP流量。所有其他流量被視為非IP，包括具有選項的IP，例如子網訪問協定(SNAP)封裝的IP和IPv6。
- 對於非IP資料包，「match access group」是唯一的分類方法，因為您無法匹配非IP流量的DSCP。媒體存取控制(MAC)存取清單(ACL)用於此目的；可以根據源MAC地址、目標MAC地址和EtherType來匹配資料包。無法將IP流量與MAC ACL相符，因為交換器會區分IP流量和非IP流量。

配置和監控管制

要在Cisco IOS中配置管制，必須執行以下步驟：

1. 定義監察器（用於聚合監察器）
2. 定義標準以選擇流量進行管制
3. 定義類對映以使用定義的條件選擇流量
4. 使用類定義服務策略並將策略應用於指定的類
5. 將服務策略應用於埠

支援以下兩種型別的策略器：

- 命名聚合
- 個人

命名的聚合策略器控制從同一策略內的所有類到應用該策略的所有類所組合的流量。不支援跨不同介面的聚合管制。

注意：聚合策略器不能應用於多個策略。如果是，則會顯示以下錯誤消息：

```
QoS: Cannot allocate policer for policy map <policy name>
```

請考慮以下示例：

連線埠GigabitEthernet0/3有一個流量產生器，會傳送約17 Mbps的UDP流量，目的地連線埠111。還有來自連線埠20的TCP流量。您希望將這兩個流量串流管製為1 Mbps，且必須捨棄多餘的流量。以下範例顯示如何完成此操作：

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

第一個示例使用命名聚合管制器。與命名策略器不同，單個策略器會針對應用它的每個類分別策略流量。單個策略器是在策略對映配置中定義的。在本示例中，兩種型別的流量由兩個單獨的策略器管制；cl_udp111被管製為每8K突發1 Mbps，cl_tcp20被管製為每32K突發512 Kbps:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
```

```
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

以下命令是用來監控管製作業的：

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

注意：預設情況下，沒有每個DSCP的統計資訊。Catalyst 3550最多支援八個不同的DSCP值的每個介面、每個方向的統計資訊收集。當您發出**mls qos monitor**命令時，會對此進行設定。為了監控DSCP 8、16、24和32的統計資訊，您必須發出以下**per-interface**命令：

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

註：mls qos monitor dscp 8 16 24 32命令將show mls qos int g0/3 statistics命令的輸出更改為以下內容：

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a        n/a      0          0
    16: 0             n/a        n/a      0          0         ? per DSCP statistics
    24: 15239542      n/a        n/a      0          0
    32: 539289117     n/a        n/a      536486430  0
Others: 1983055       n/a        n/a      1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

以下是範例中欄位的說明：

- **Incoming** — 顯示從每個方向到達的資料包數量
- **NO_change** — 顯示有多少資料包受信任（例如QoS級別未更改）
- **Classified** — 顯示分類後為此內部DSCP分配了多少資料包
- **Policed** — 顯示有多少資料包被策略降級；降級前顯示的DSCP。
- **Dropped** — 顯示管制丟棄的資料包數

請注意以下特定於實施的注意事項：

- 如果在發出**mls qos monitor**命令時配置了八個DSCP值，則在發出**show mls qos int statistics**命令時看到的其他計數器可能顯示不充分的資訊。
- 沒有特定命令可驗證每個監察器的已提供或傳出流量速率。
- 由於計數器是從硬體順序檢索的，因此計數器可能會不能正確累加。例如，受管制、分類或丟棄的資料包數量與傳入資料包的數量可能略有不同。

配置和監控標籤

要配置標籤，必須執行以下步驟：

1. 定義流量分類標準
2. 定義要按照先前定義的標準分類的流量類
3. 建立將標籤操作和策略操作附加到已定義類的策略對映
4. 將相應的介面配置為信任模式
5. 將策略對映應用於介面

在本示例中，您希望傳入IP流量傳送到主機192.168.192.168，該主機標有IP優先順序6，並被限製為1 Mbps;必須將多餘流量降級為IP優先順序2:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

發出了相同的**show mls qos interface statistics** 命令以監控標籤。示例輸出和影響見於本文檔的一節。

如何使用單個監察器對所有介面流量進行分類

在Catalyst 3550上，不支援**match interface**命令，且每個類別對映只允許一個match命令。此外，Catalyst 3550不允許IP流量與MAC ACL相符。因此，IP和非IP流量必須使用兩個單獨的類對映進行分類。因此，很難對進入介面的所有流量進行分類，並使用單個監察器來管制所有流量。通過這

裡的示例配置，您可以完成此操作。在此配置中，IP和非IP流量與兩個不同的類對映匹配。但是，每個控制器對兩個流量都使用公共監察器。

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

相關資訊

- 在Catalyst 3550上配置QoS
- 服務品質支援頁面
- LAN 交換支援頁面
- LAN 產品支援頁面
- 技術支援與文件 - Cisco Systems